

Supplemental Report: BlackBerry Z10 Apps and Privacy

Table of Contents

Introduction	2
Phase 1: Literature Review	2
Phase 2: Permissions Study and App Selection.....	2
Hardware and Software	2
BlackBerry World (App Store) Survey.....	3
App Selection and Criteria	3
Free BlackBerry Z10 Apps	3
Paid BlackBerry Z10 Apps	3
Permission Discovery and Types.....	3
Permissions by Application.....	4
BlackBerry Z-10 Selected Free Apps	4
BlackBerry Z-10 Selected Paid Apps	5
Phase 3: In-Depth Analysis	5
In-Depth Analysis Methodology	5
Connecting to a PC-Based Wireless Hotspot with Connectify Hotspot	6
Man in the Middle Data Flow Analysis.....	6
Analysis Findings	6
BeWeather 10 Pro	7
Dictionary.com	7
GPS Maps for Google Maps	7
Conclusions	8
Appendix: Blackberry Z10 Raw Data.....	9
Phone Information.....	9
Free Apps	9
WhatsApp.....	9
Facebook	10
CB10.....	13
Waze.....	15
Whip.....	15
Paid Apps	16
BeWeather Pro 10.....	16
GadgetBox	17
GPS Maps for Google Maps.....	17
Police Scanner Radio	20
Dictionary.com.....	21

Introduction

This document is intended to supplement the project entitled *An Investigation of the Role of Smartphone Application Permissions in Risks to End User Privacy*, by adding information that, while not originally specified in the project description, was deemed critically relevant. This supplement is a companion to the project's report, entitled "Smartphone Apps, Permissions and Privacy: Concerns and Next Steps," referred to as the "primary report," elsewhere in this document.

When the project began in April 2012, smartphone manufacturer BlackBerry was known as Research In Motion (RIM), and its phones utilized BlackBerry OS versions 7 and earlier. On January 30, 2013, RIM changed its name to BlackBerry. More importantly, the company introduced a new line of smartphones utilizing the BlackBerry 10 OS. The BlackBerry 10 OS was developed based on the QNX software kernel, making it significantly different from past BlackBerry platforms that used the old BlackBerry OS kernel. BlackBerry 10 handles, declares, classifies and manages permissions differently than its predecessors. The new operating system was initially released on the new touchscreen-only BlackBerry Z10; as of this writing, the company has plans to release the BlackBerry Q10, a device with a hardware keyboard that also runs the BlackBerry 10 OS.

BlackBerry is a Canadian company with a significant share of the Canadian smartphone market, making continued studies of its offerings relevant to the project, especially since BlackBerry phones have long been employed in business and government both for their perceived role as workplace devices, and their reputation for security. Therefore, even though the project was outlined before the BlackBerry 10 OS release, this supplemental information is relevant to the project's goals.

In order to provide this information within the time and budget constraints imposed by the BlackBerry 10 OS's January 30, 2013 release date, Tekdesk researchers utilized a truncated version of the processes used to analyze app permissions and their privacy implications on other platforms. This supplement describes that process, and explains Tekdesk's findings.

Phase 1: Literature Review

Tekdesk researchers did not conduct a formal literature review, but did study media reports and BlackBerry's developer resources when necessary.

Phase 2: Permissions Study and App Selection

Researchers modified the methodology in the primary report by selecting BlackBerry 10 apps for in-depth review before conducting the initial permissions study. Thus, the permissions study was limited to apps selected for in-depth study.

Hardware and Software

Researchers used a BlackBerry Z10 smartphone running the BlackBerry 10 operating system. Researchers applied updates to the operating system when prompted by the device.

BlackBerry World (App Store) Survey

On March 27, 2013, researchers captured a list of the 50 most popular free and 50 most popular paid apps for the BlackBerry Z10 from the BlackBerry World app store. At the time of capture, BlackBerry World was capable of filtering results by device. Unlike the primary report, this supplemental effort did not record permissions from all 100 apps.

App Selection and Criteria

Researchers selected apps for in-depth analysis before performing permissions analysis, and limited permissions analysis to those selected apps. Researchers selected the following apps according to the criteria listed beside them.

Free BlackBerry Z10 Apps

- **WhatsApp:** Selected due to known issues, identified in the primary report, in other platforms and reported in the media.
- **Facebook:** Selected due to the popularity and wide ranging privacy implications of this social network.
- **CB10:** Selected due to its popularity, and the fact that it is an app produced by Crackberry.com, a Canadian media site for BlackBerry smartphones.
- **Waze:** Selected due to the fact that it combines location-based and social features—two characteristics of apps that often present privacy risks.
- **Whip:** Selected because free recreational apps are often associated with suspicious permissions and behavior. We found this one in particular suspicious because we could not identify a clear business model/profit motive for its release.

Paid BlackBerry Z10 Apps

- **BeWeather Pro 10:** Selected for its geolocation capabilities, and as the most popular paid app as of the March 27, 2013 survey.
- **Gadget Box:** Selected as a popular, multi-function app that requires special access to the smartphone's camera and other capabilities.
- **GPS Maps for Google Maps:** Selected due to its geolocation features, and because it is a third party app using the Google Maps API.
- **Police Scanner Radio:** Selected due to the nature of the app and because it has location-based capabilities.
- **Dictionary.com:** Selected due to known privacy issues reported in other platforms.

Permission Discovery and Types

BlackBerry devices do not list permissions in the BlackBerry World store. Apps must be installed to discover their permissions. Apps listed on the BlackBerry World website can be found and downloaded from within the BlackBerry World app by either searching by name, or using a BlackBerry device's camera to scan the app's QR code on its webpage listing.

Inspecting permissions across multiple apps generated the following permissions list:

- Internet
- Location

- Contacts
- Email and PIN Messages
- Shared Files
- GPS Location
- Microphone
- Camera
- Connect to BBM
- BBM Contact Invites
- Profile Updates

Permissions appear when the app is first downloaded. After that point, they can be viewed in the device by going to **Settings>Security and Privacy>Application Permissions**.

Permissions by Application

Downloaded apps possessed the following permissions, listed by app.

BlackBerry Z-10 Selected Free Apps

App	WhatsApp	Facebook	CB10	Waze	Whip
Function	Messaging	Facebook social network	BlackBerry news from Crackberry.com	Navigation with social networking for traffic reporting	Makes a whipping sound.
Internet	No	No	No	Yes	Not listed
Location	Yes	Yes	No	No	Not listed
Contacts	Yes	No	No	Yes	Not listed
Email and PIN Messages	Yes	No	No		Not listed
Shared Files	Yes	Yes	Yes	Yes	Not listed
GPS Location	No	No	No	Yes	Not listed
Microphone	No	No	No	Yes	Not listed
Camera	No	No	No	Yes	Not listed
Connect to BBM	No	No	Yes	No	Not listed
BBM Contact Invites	No	No	Yes	No	Not listed
Profile Updates	No	No	Yes	No	Not listed
Notes	Uses internet, but no internet permission. Issues reported in other platforms.	Uses internet, but no internet permission.	Uses internet, but no internet permission. Why does it need BBM access?	Wide	No suspicious data sent, but does not show up in Settings>Security and Privacy>Application Permissions

BlackBerry Z-10 Selected Paid Apps

App	BeWeather 10 Pro	Gadget Box	GPS Maps for Google Maps	Police Scanner Radio	Dictionary.com
Function	Weather app	Multiple uses; included level, height estimator, etc.	Google maps-based third party application.	Police/Emergency services scanner	Dictionary
Internet	No	No	No	No	No
Location	Yes	Yes	No	No	No
Contacts	No	No	No	No	No
Email and PIN Messages	No	No	No	No	No
Shared Files	Yes	No	No	No	No
GPS Location	Yes	Yes	Yes		
Microphone			No		
Camera		Yes	No	Yes	
Connect to BBM	Yes	No	No	No	Yes
BBM Contact Invites	Yes	No	No	No	Yes
Profile Updates		No	No	No	Yes
Device Identifying Information	Yes	No	No	No	Yes
Notes	Uses internet, but no internet permission.	Uses internet, but no internet permission.	Uses internet, but no internet permission. Doesn't seem to customize itself based on location.	Uses internet, but no internet permission. Doesn't seem to customize itself based on location.	Uses internet, but no internet permission. Why does it need DID? Known privacy issues in other platforms.

Phase 3: In-Depth Analysis

Just as for the primary report, Tekdesk employed Dot Net Can, Inc., a Toronto, Ontario based software development firm, to develop a method for in-depth analysis, and help select apps suitable for in-depth study using that method. Dot Net Can developer Chad McGrath applied the Man in the Middle (MITM) data flow analysis originally developed for the study detailed in the primary report, to the selected BlackBerry Z10 apps.

In-Depth Analysis Methodology

Tekdesk's Man in the Middle analysis method used the following steps:

1. Connect devices to a PC-based Wi-Fi hotspot.
2. Conduct Man in the Middle (MITM) data flow analysis
3. Analyze Results
4. Compare to Permissions

Connecting to a PC-Based Wireless Hotspot with Connectify Hotspot

Researchers used Connectify Hotspot (<http://www.connectify.me/hotspot/>) to convert a PC wireless card into a Wi-Fi hotspot, relaying network connections in the same fashion as hardware router. This allowed it to be analyzed as it passed through a PC with the following specifications:

- 3rd generation Intel Core i5-3210M processor (3MB Cache, up to 3.1GHz w/Turbo Boost 2.0)
- 12 GB DDR3 RAM
- Wired Ethernet: Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6.20)
Wireless Card: Centrino-Wireless-N-2230
- OS: 64 Bit Windows 7 Home Premium Service Pack 1

Researchers connected the BlackBerry Z10 to the hotspot created by Connectify to study its data flows.

Man in the Middle Data Flow Analysis

To monitor these data flows using MITM methods, researchers employed the following additional tools:

- **Burp Proxy** (<http://portswigger.net/burp/proxy.html>) is an intercepting proxy server used for MITM data analysis.
- **Fiddler** (<http://www.fiddler2.com/fiddler2/>) is a web debugging proxy that monitors http and https traffic from both applications and devices.

Researchers installed SSL certificates to permit monitoring by each application. Installed on the same PC as the Connectify-enabled hotspot, they performed MITM captures of traffic passing to and from the BlackBerry Z10 while each app went through the following states:

- During and immediately after app installation.
- With the app installed, but not activated by the user.
- With the app running in the background.
- With the app running and being used for its primary purpose for approximately 10 minutes.
- In additional scenarios, when warranted to the app's nature, behaviour in initial studies, or insights from other literature.

In addition to analyzing data flows, researchers compared them and each app's general behaviour to their listed permissions.

Analysis Findings

Researchers discovered three apps with privacy-related issues. As per the primary report, this supplement does not include non-notable results. Apps that are not detailed below were not observed to handle user data in an insecure or suspicious fashion.

BeWeather 10 Pro

Function: Drawing information from the Weather Underground website, BeWeather 10 Pro provides weather information to users. It uses animated graphics to present this information in a visually attractive fashion.

Privacy Policy: <http://www.bellshare.com/privacy.php>. Note that this policy does not specifically mention the app, but appears as a general policy on the developer's support website.

Privacy Risks: Data flow analysis discovered that the app transmits the device's ID (or PIN) over an unencrypted connection. This would allow a third party to capture its PIN. PINs are used for multiple functions by apps, as well as to identify messages sent through the BlackBerry Messenger service. This could allow a third party to send the user unwanted messages.

The app also transmits geolocation data across the same connection, associating it with the PIN. This location information is presumably being used to deliver accurate local weather results. Besides the potential danger of associating a PIN with a physical location, the geolocation data is in itself unnecessarily accurate for the app's function—it doesn't need to know a user's location to within a few metres to deliver accurate weather results.

Other Factors: None.

Dictionary.com

Function: Drawing from Dictionary.com, this app provides word definitions, a word of the day feature and the ability to share dictionary definitions with others via BlackBerry Messenger.

Privacy Policy: <http://thesaurus.com/privacy>

Privacy Risks: Data flow analysis discovered that the app transmits the device's ID (or PIN). It is not clear why this is necessary. To send a message include app content, app servers should not require the PIN, as the message is being sent from the device, not from the app's servers.

Other Factors: None.

GPS Maps for Google Maps

Function: This app uses the Google Maps API to provide third party access to Google Maps' functions.

Privacy Policy: This app has no support site, and its privacy policy could not be located. Developer Smashing Appz Studioz, refers support requests to an email address smashingappzstudioz@gmail.com.

Privacy Risks: The app transmits geolocation data over an unencrypted http connection. During tests, it transmitted incorrect data, but an update or fix would make this a true privacy

concern. The lack of a privacy policy or developer website also raises questions about accountability.

Other Factors: The app does not appear to function properly. It transmitted an incorrect, physically impossible set of GPS coordinates.

Conclusions

Findings from our study of the BlackBerry Z10 are consistent with findings from the primary report, and our recommendations remain the same. The issues we found with lack of encryption and too-accurate geolocation data are the same as those reported for apps on other platforms.

The BlackBerry device ID/PIN adds an additional issue, specific to BlackBerry devices. This was not apparent in our studies of other BlackBerry devices in the primary report, possibly because our test devices would not allow us to use an https proxy, limiting our ability to view data flows. Irresponsible handling of a user's PIN could be used to gather private information, or allow unwanted messages through BlackBerry Messenger.

This issue does not mean the Z10 is especially flawed. In fact, researchers appreciated the fact that users could control app permissions at will, to a relatively fine degree. The interface for doing so (in device Settings) was easier to use, and each permission included an explanation for the layperson. Only the Internet permission was problematic. Several apps did not request it despite clearly using internet-based resources.

Unfortunately, it is still impossible to view app permissions before download, the way one can when using Google Play for an Android device. If BlackBerry listed permissions in its BlackBerry World store, we would consider it to use the best practices out of the platforms we monitored. Currently, we cannot say that it is superior or inferior to the other platforms in terms of protecting user privacy, however.

Appendix: Blackberry Z10 Raw Data

Phone Information

- **Name:** BlackBerry-3386
- **Serial Number:** 0616-6414-1461
- **MAC Address:** 406f2a2ff493
- **Software Version:** 10.0.10.85
- **Model:** STL100-3
- **ID:** 89302610402010654477
- **IMEI:** 352921050729277
- **ICC ID:** 893026104020106544777058750955

Free Apps

WhatsApp

Notes

- Intermittent proxy connection.

GET

/v2/code?cc=1&in=7058750955&lg=en&lc=US&id=%96%da%a0%27%f3%22%d6%c5%14%07%58%3c%2e%ba%72%a6%01%7b%89%cc&method=self&reason=same-device-fail&token=0a177dbb264d5243b289a73550806f5e&mnc=610&mcc=302 HTTP/1.1

User-Agent: WhatsApp/2.9.4662 BlackBerry/10.0.10.672 Device/STL100-3

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

Host: v.whatsapp.net

GET

/v2/register?cc=1&in=7058750955&lg=en&lc=US&id=%96%da%a0%27%f3%22%d6%c5%14%07%58%3c%2e%ba%72%a6%01%7b%89%cc&code=TRyUglli1ekJJ%2FB8jTsBz9k2s9w%3D HTTP/1.1

User-Agent: WhatsApp/2.9.4662 BlackBerry/10.0.10.672 Device/STL100-3

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

Host: v.whatsapp.net

Facebook

Notes

- No fresh install.
- Everything is sent over https. That's good.

GET

/fql?access_token=BAADlaSJt7ZC4BAIAkroQBq1quWZCFEFi3vLZBPiU0fSgTThbqRHiuJ1IDJZB3LhZCaU6pUEqZBNKcUHTvEr8nXpsWKWktrRTsJDCCNbrtAjQZDZD&locale=en_US&q=%7B%0A%20%20%22friends%22%20%3A%20%22SELECT%20uid%2%2Cis_removed%20FROM%20friend_sync%20WHERE%20uid1%20%3D%20me%28%29%20and%20update_time%20%3E%3D%201365163483%22%2C%0A%20%20%20%22ranks%22%20%3A%20%22SELECT%20uid%2%2Ccommunication_rank%20FROM%20friend%20WHERE%20uid1%20%3D%20me%28%29%20AND%20uid%20IN%20%28SELECT%20uid%20from%20%23friends%29%22%2C%0A%20%20%20%22users%22%20%3A%20%22SELECT%20uid%2Cname%2Cfirst_name%2Cmiddle_name%2Clast_name%2Ccontact_email%2Cphones%2Cis_pushable%2Chas_messenger%2Cbirthday_date%20FROM%20user%20WHERE%20uid%20IN%20%28SELECT%20uid%20from%20%23friends%29%22%0A%7D%0A HTTP/1.1

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

User-Agent: Mozilla/5.0

Host: graph.facebook.com

GET

/fql?access_token=BAADlaSJt7ZC4BAIAkroQBq1quWZCFEFi3vLZBPiU0fSgTThbqRHiuJ1IDJZB3LhZCaU6pUEqZBNKcUHTvEr8nXpsWKWktrRTsJDCCNbrtAjQZDZD&locale=en_US&q=SELECT%20unseen_count%20FROM%20unified_thread_count%20WHERE%20folder%3D%27inbox%27 HTTP/1.1

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

User-Agent: Mozilla/5.0

Host: graph.facebook.com

GET

/fql?access_token=BAADlaSjt7ZC4BAIZAkroQBq1quWZCFEFi3vLZBPiU0fSgTThbqRHuJ1IDJZB3LhZCaU6pUEqZBNKcUHTvEr8nXpsWKWktrRTsJDCCNbrtAjQZDZD&locale=en_US&q=%7B%20%22query0%22%20%3A%20%22SELECT%20uid_from%2C%20time%2C%20unread%20FROM%20friend_request%20WHERE%20uid_to%20%3D%20me%28%29%20AND%20%28unread%20%3D%201%20OR%20time%20%3E%200%29%20LIMIT%20100%22%2C%20%22query1%22%20%3A%20%22SELECT%20uid_from%20FROM%20friend_request%20WHERE%20uid_to%20%3D%20me%28%29%20AND%20time%20%3C%3D%200%20AND%20time%20%3E%3D%200%20LIMIT%20100%22%2C%20%22query2%22%20%3A%20%22SELECT%20uid%2C%20name%2C%20affiliations.name%20FROM%20user%20WHERE%20uid%20IN%20%28SELECT%20uid_from%20FROM%20%23query0%29%20LIMIT%20100%22%2C%20%22query3%22%20%3A%20%22SELECT%20id%2C%20url%2C%20size%20FROM%20square_profile_pic%20WHERE%20size%20IN%20%28148%29%20AND%20id%20IN%20%28SELECT%20uid%20FROM%20%23query2%29%22%20%7D HTTP/1.1

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

User-Agent: Mozilla/5.0

Host: graph.facebook.com

GET

/fql?access_token=BAADlaSjt7ZC4BAIZAkroQBq1quWZCFEFi3vLZBPiU0fSgTThbqRHuJ1IDJZB3LhZCaU6pUEqZBNKcUHTvEr8nXpsWKWktrRTsJDCCNbrtAjQZDZD&locale=en_US&q=%7B%20%22child_query%22%20%3A%20%22SELECT%20parent_post_id%2Cpost_id%2Capp_id%2Csource_id%2Cupdated_time%2Ccreated_time%2Ctribution%2Cactor_id%2Ctarget_id%2Cvia_id%2Cimplicit_place%2Cmessage%2Cwith_tags%2Capp_data%2Caction_links%2Cattachment%2Ccomments%2Clikes%2Cplace%2Cprivacy%2Ctype%2Cmessage_tags%2Cdescription%2Cdescription_tags%2Ctagged_ids%2Cview_time_position%20FROM%20stream%20WHERE%20is_hidden%20%3D%200%20AND%20updated_time%20%3E%201364925373%20AND%20filter_key%20in%20%28SELECT%20filter_key%20FROM%20stream_filter%20WHERE%20uid%3Dme%28%29%20AND%20type%3D%27newsfeed%27%29%20AND%20parent_post_id%20IN%20%28SELECT%20post_id%20FROM%20%23post_query%29%20ORDER%20BY%20created_time%20DESC%20limit%2030%22%2C%20%20%20%20%22place_page_query%22%20%3A%20%22SELECT%20page_id%2Cname%2Ccategories%2Cpic_square%2Ctype%2Clocation%20FROM%20page%20WHE

RE%20page_id%20IN%20%28SELECT%20place%20FROM%20%23post_query%29%20OR%20page_id%20IN%20%28SELECT%20place%20FROM%20%23child_query%29%22%2C%0A%20%20%20%22post_query%22%20%3A%20%22SELECT%20parent_post_id%2Cpost_id%2Capp_id%2Csou
rce_id%2Cupdated_time%2Ccreated_time%2Ctribution%2Cactor_id%2Ctarget_id%2Cvia_id%
2Cimplicit_place%2Cmessage%2Cwith_tags%2Capp_data%2Caction_links%2Cattachment%2Cco
mments%2Clikes%2Cplace%2Cprivacy%2Ctype%2Cmessage_tags%2Cdescription%2Cdescriptio
n_tags%2Ctagged_ids%2Cview_time_position%20FROM%20stream%20WHERE%20is_hidden%
20%3D%200%20AND%20updated_time%20%3E%201364925373%20AND%20filter_key%20in%
20%28SELECT%20filter_key%20FROM%20stream_filter%20WHERE%20uid%3Dme%28%29%20
AND%20type%3D%27newsfeed%27%29%20AND%20parent_post_id%3D%27%27%20ORDER%2
0BY%20created_time%20DESC%20limit%2015%22%2C%0A%20%20%20%22profile_query%22%
20%3A%20%22SELECT%20id%2Cname%2Ctype%2Cpic_square%20FROM%20profile%20WHERE
%20id%20IN%20%28SELECT%20actor_id%20FROM%20%23post_query%29%20OR%20id%20IN
%20%28SELECT%20target_id%20FROM%20%23post_query%29%20OR%20id%20IN%20%28SEL
ECT%20tagged_ids%20FROM%20%23post_query%29%20OR%20id%20IN%20%28SELECT%20via
_id%20FROM%20%23post_query%29%20OR%20id%20IN%20%28SELECT%20implicit_place%20
FROM%20%23post_query%29%20OR%20id%20IN%20%28SELECT%20likes.friends%20FROM%2
0%23post_query%29%20OR%20id%20IN%20%28SELECT%20likes.sample%20FROM%20%23pos
t_query%29%20OR%20id%20IN%20%28SELECT%20actor_id%20FROM%20%23child_query%29
%20OR%20id%20IN%20%28SELECT%20target_id%20FROM%20%23child_query%29%20OR%20i
d%20IN%20%28SELECT%20tagged_ids%20FROM%20%23child_query%29%20OR%20id%20IN%
20%28SELECT%20via_id%20FROM%20%23child_query%29%20OR%20id%20IN%20%28SELECT
%20implicit_place%20FROM%20%23child_query%29%20OR%20id%20IN%20%28SELECT%20lik
es.friends%20FROM%20%23child_query%29%20OR%20id%20IN%20%28SELECT%20likes.saml
e%20FROM%20%23child_query%29%22%0A%7D%0A HTTP/1.1

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

User-Agent: Mozilla/5.0

Host: graph.facebook.com

GET

/fql?access_token=BAADlaSJt7ZC4BAIAkroQBq1quWZCFEFi3vLZBPiU0fSgTThbqRHiuJ1IDJZB3Lh
ZCaU6pUEqZBNKcUhtvEr8nXpsWKWktrRTsJDCCNbrtAjQZDZD&locale=en_US&q=SELECT%20uns
een_count%20FROM%20unified_thread_count%20WHERE%20folder%3D%27inbox%27
HTTP/1.1

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

User-Agent: Mozilla/5.0

Host: graph.facebook.com

GET

/method/facebook.fql.multiquery?access_token=BAACiejtbIPABAJ37Emmmu1tCSqRFinsmFULx9jQimRDzAZCr0KzZAJZBEi2uK34wSOYFPjOogDDeY2AFc2SqQckLxbUcwlyz2dRZA9ylvc5Va4PNWrpzg5laWOT3bZACLPiGzkf4k7BVuECC7rU2xxZBMW2TtwWNtGPhAlsoyrJtg0eK8jkGRQ&format=JSON&queries=%7B%22getMessage%22%3A+%22SELECT+message_id%2C+thread_id%2C+author_id%2C+body%2C+created_time%2C+attachment+FROM+message+WHERE+thread_id+IN+%28SELECT+thread_id+from+%23getThread%29%22%2C+%22getThread%22%3A+%22SELECT+thread_id%2C+folder_id%2C+subject%2C+recipients%2C+updated_time%2C+parent_thread_id%2C+message_count%2C+snippet%2C+snippet_author%2C+object_id%2C+unread+FROM+thread+WHERE+%28folder_id%3D1+OR+folder_id%3D0%29+AND+updated_time+%3E+1365355586+ORDER+BY+updated_time+DESC+LIMIT+0%2C+20%22%2C+%22getProfileNames%22%3A+%22SELECT+id%2C+name+FROM+profile+WHERE+id+IN+%28SELECT+snippet_author%2C+recipients+FROM+%23getThread%29%22%2C+%22getMyProfile%22%3A+%22SELECT+id%2C+name+FROM+profile+WHERE+id+%3D+636131557%22%7D HTTP/1.1

Host: api.facebook.com

accept-encoding: gzip, deflate

user-agent: Python-httpplib2/0.7.2 (gzip)

CB10

Notes

- Connects to BBM.
- Sends out PIN over https.

GET /mobile_app/feed?section=reviews HTTP/1.1

User-Agent: MNAPP(CB10) 1.0 BB10 Mobile

Cookie: PassportLocalSession=; PassportSession=; PassportSessionDate=; SESS6e06694a939e38f77631a183270c10bc=; SESSa5e0e8ed865b160813ab8f1aba9d9b58=; cbpassword=; cbsessionhash=; cbuserid=

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

Host: m.crackberry.com

GET /mobile_app/feed?page=0 HTTP/1.1

User-Agent: MNAPP(CB10) 1.0 BB10 Mobile

Cookie: PassportLocalSession=; PassportSession=; PassportSessionDate=;
SESS6e06694a939e38f77631a183270c10bc=; SESSa5e0e8ed865b160813ab8f1aba9d9b58=;
cbpassword=; cbsessionhash=; cbuserid=

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

Host: m.crackberry.com

POST /mobiquo/mobiquo.php HTTP/1.1

Content-Type: text/xml

User-Agent: MNAPP(CB10) 1.0 BB10 Mobile

Cookie: PassportLocalSession=; PassportSession=; PassportSessionDate=;
SESS6e06694a939e38f77631a183270c10bc=; SESSa5e0e8ed865b160813ab8f1aba9d9b58=;
cbpassword=; cbsessionhash=; cbuserid=

Content-Length: 80

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

Host: forums.crackberry.com

<?xml version="1.0"?><methodCall><methodName>get_forum</methodName></methodCall>

POST

/ClientAPI/usfdownload?contentid=25225877&licensetypeid=1&clientver=4.2&model=0x85002
40a&os=10.0.10&countryid=36&carrierid=109¤tmcc=302&pin=24c13386 HTTP/1.1

Accept-Encoding: gzip

Accept-Language: en_US

Content-Language: en_US

Content-Type: application/x-www-form-urlencoded

User-Agent: AppWorld/4.2.1.109

Authorization: AQ%3AdDn0rLJgA7SB0UgMEGx6dyhUJwmQfq-
tzS7lxl2uEZ0%3ALhojGi6DE6G78z4qcAsQdQ%3A1URnU7CbK7ei6XUHFT6FOkNo1PrcBlanzyy4irP
cJPFatpc6711-QpF4CiOzA1Qck2iObOI07ZSCgOZbGp5BkDD_6T-4pMo3gVYiGZy1Jf4RGAjmKfomJ-
pkBWOzBKHGKipIMXU0koAIGZI0BzCOWsnmgtidhbQ6ZSXoduTHQcJFLC69jaSYMlz8KnqLbCwGSF
Jmi3E_OybGS_xLwtq9GYS7yPWGZv1WaPRDG6qCFS8pzuvd2lphIYBrXmDvtMhBC9ZFvi-
bcJ_iunquLGa8S2_-mfQvjsqaPKmRW8-JiSJ-YJ49Q7u5pR955-
UYpYqtp6NAitBgiEmQupXsPwcDjpfmq3xNoeJnpvNDfC8LuiKDLWyJydB-
0duYNIVufUX14zl1bpFWYCOrvleqr7EC3Ftc9TqOytXBDVsUFI4qxZDt2VuQ3o4iElhya2yLpgluz_pFy
AFEZoejQkfn0Abb-
CD3D8X1eiTo8LpVoyUsgwKOPQfPW8xP6Y1GHXDRM9GkmG_bn8Zgl3wSEejCwUSBXoMFNnGI-
mssCL8Y0utWUsY

Content-Length: 0

Connection: Keep-Alive

Host: appworld.blackberry.com

Waze

Notes

- No data.
- Intermittent connection to Proxy—it probably defeated the MITM attack.

Whip

Notes

- Doesn't appear to use personal information.

GET /static/img/artistimages/00/010/801/0001080159_300.jpg HTTP/1.1

User-Agent: AppWorld/4.2.1.109

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

Host: cdn.7static.com

Paid Apps

BeWeather Pro 10

Notes

- Sends DID/PIN over http.

GET

/api.v2h.php?format=json&action=getForecast&returnnearby=1&location=gps&units=english&windunits=mph&lat=43.6417&lon=-79.4052 HTTP/1.1

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

User-Agent: Mozilla/5.0

Host: xmlrpc1.berryweather.com

GET /api.v2h.php?format=json&action=getAdvisory&location=gps&lon=-79.4052&lat=43.6417&push=21600&device=blackberry&deviceid=24C13386&lat=43.6417&lon=-79.4052 HTTP/1.1

Connection: Keep-Alive

Accept-Encoding: gzip

Accept-Language: en-US,*

User-Agent: Mozilla/5.0

Host: xmlrpc1.berryweather.com

GET /maps/api/js?key=AlzaSyAsVFttdZ-2ukqOORTFb9gpw9vrJxroPp0&sensor=false HTTP/1.1

Accept-Encoding: gzip,deflate

Accept-Language: en-US,en;q=0.8

User-Agent: Mozilla/5.0 (BB10; Touch) AppleWebKit/537.10+ (KHTML, like Gecko)
Version/10.0.10.672 Mobile Safari/537.10+

Accept: */*

Referer: http://xmlrpc.berryweather.com/map.php?lat=43.64170575&lon=-79.4053311

Host: maps.googleapis.com

Connection: keep-alive

GadgetBox

Notes

- No outgoing data.

GPS Maps for Google Maps

Notes

- Sends GPS latitude/longitude info, but it seems to be wrong
- Sends GPS location over http.

GET

/maps/api/js?libraries=places&key=AlzaSyBeQBZMsbtixmLiKka631KHT78EUZCNfn0&sensor=true HTTP/1.1

Accept-Encoding: gzip,deflate

Proxy-Connection: Keep-Alive

Date: Dec 23 2010, 13:30 GMT-5

Accept-Language: en-US,en;q=0.8

User-Agent: Mozilla/5.0 (BB10; Touch) AppleWebKit/537.10+ (KHTML, like Gecko)
Version/10.0.10.672 Mobile Safari/537.10+

Accept: */*

Host: maps.googleapis.com

Connection: keep-alive

HTTP/1.1 200 OK

Content-Type: text/javascript; charset=UTF-8

Date: Sun, 07 Apr 2013 20:32:54 GMT

Expires: Sun, 07 Apr 2013 21:02:54 GMT

Cache-Control: public, max-age=1800

Vary: Accept-Language

Access-Control-Allow-Origin: *

Server: mafe

Content-Length: 2778

X-XSS-Protection: 1; mode=block

X-Frame-Options: SAMEORIGIN

```
window.google = window.google || {};
```

```
google.maps = google.maps || {};
```

```
(function() {
```

```
function getScript(src) {
```

```
    document.write('<' + 'script src="' + src + '"' +  
        ' type="text/javascript"><' + '/script>');
```

```
}
```

```
var modules = google.maps.modules = {};
```

```
google.maps.__gjsload__ = function(name, text) {
```

```

modules[name] = text;

};

google.maps.Load = function(apiLoad) {

delete google.maps.Load;

apiLoad([0.009999999776482582,[[["http://mt0.googleapis.com/vt?lyrs=m@212000000\u0026src=api\u0026hl=en-US\u0026","http://mt1.googleapis.com/vt?lyrs=m@212000000\u0026src=api\u0026hl=en-US\u0026"],null,null,null,null,"m@212000000"],[["http://khm0.googleapis.com/kh?v=126\u0026hl=en-US\u0026","http://khm1.googleapis.com/kh?v=126\u0026hl=en-US\u0026"],null,null,null,1,"126"],[["http://mt0.googleapis.com/vt?lyrs=h@212000000\u0026src=api\u0026hl=en-US\u0026","http://mt1.googleapis.com/vt?lyrs=h@212000000\u0026src=api\u0026hl=en-US\u0026"],null,null,"imgtp=png32\u0026",null,"h@212000000"],[["http://mt0.googleapis.com/vt?lyrs=t@130,r@212000000\u0026src=api\u0026hl=en-US\u0026","http://mt1.googleapis.com/vt?lyrs=t@130,r@212000000\u0026src=api\u0026hl=en-US\u0026"],null,null,null,null,"t@130,r@212000000"],null,null,[["http://cbk0.googleapis.com/cbk?","http://cbk1.googleapis.com/cbk?"]],[["http://khm0.googleapis.com/kh?v=73\u0026hl=en-US\u0026","http://khm1.googleapis.com/kh?v=73\u0026hl=en-US\u0026"],null,null,null,null,"73"],[["http://mt0.googleapis.com/mapsIt?hl=en-US\u0026","http://mt1.googleapis.com/mapsIt?hl=en-US\u0026"]],[["http://mt0.googleapis.com/mapsIt/ft?hl=en-US\u0026","http://mt1.googleapis.com/mapsIt/ft?hl=en-US\u0026"]],[["http://mt0.googleapis.com/vt?hl=en-US\u0026","http://mt1.googleapis.com/vt?hl=en-US\u0026"]],[["http://mt0.googleapis.com/mapsIt/loom?hl=en-US\u0026","http://mt1.googleapis.com/mapsIt/loom?hl=en-US\u0026"]],[["https://mts0.googleapis.com/mapsIt?hl=en-US\u0026","https://mts1.googleapis.com/mapsIt?hl=en-US\u0026"]],[["https://mts0.googleapis.com/mapsIt/ft?hl=en-US\u0026","https://mts1.googleapis.com/mapsIt/ft?hl=en-US\u0026"]],["en-US","US",null,0,null,null,"http://maps.gstatic.com/mapfiles/","http://csi.gstatic.com","https://maps.googleapis.com","http://maps.googleapis.com"],[["http://maps.gstatic.com/intl/en_us/mapfiles/api-3/12/6c","3.12.6c"],[2728138956],1.0,null,null,null,null,1,"","places"],null,0,"http://khm.googleapis.com/mz?v=126\u0026","AlzaSyBeQBZMsbtixmLiKka631KHT78EUZCNfn0","https://earthbuilder.googleapis.com","https://earthbuilder.googleapis.com",null,"http://mt.googleapis.com/vt/icon"],loadScriptTime);

```

```
};  
  
var loadScriptTime = (new Date).getTime();  
  
getScript("http://maps.gstatic.com/cat_js/intl/en_us/mapfiles/api-  
3/12/6c/%7Bmain,places%7D.js");  
  
})();
```

Police Scanner Radio

Notes

- Sends latitude/longitude info, but doesn't seem to change how the app behaves.

GET /audio/?a=countries&type=xml&key=41230717 HTTP/1.1

Host: api.radioreference.com

Accept-Encoding: deflate, gzip

Proxy-Connection: Keep-Alive

Accept: text/xml, application/xml, application/xhtml+xml, text/html;q=0.9, text/plain;q=0.8, text/css, image/png, image/jpeg, image/gif;q=0.8, application/x-shockwave-flash, video/mp4;q=0.9, flv-application/octet-stream;q=0.8, video/x-flv;q=0.7, audio/mp4, application/futuresplash, */*;q=0.5

User-Agent: Mozilla/5.0 (X11; U; Linux i686;) AppleWebKit/533.19.4 (KHTML, like Gecko) AdobeAIR/3.1

x-flash-version: 11,1,121,108

Connection: Keep-Alive

Referer: app:/PoliceScannerRadio.swf

GET /audio/?a=states&coid=2&type=xml&key=41230717 HTTP/1.1

Host: api.radioreference.com

Accept-Encoding: deflate, gzip

Proxy-Connection: Keep-Alive

Accept: text/xml, application/xml, application/xhtml+xml, text/html;q=0.9, text/plain;q=0.8, text/css, image/png, image/jpeg, image/gif;q=0.8, application/x-shockwave-flash, video/mp4;q=0.9, flv-application/octet-stream;q=0.8, video/x-flv;q=0.7, audio/mp4, application/futuresplash, */*;q=0.5

User-Agent: Mozilla/5.0 (PlayBook; U; RIM Tablet OS 2.1.0; en-US) AppleWebKit/536.2+ (KHTML, like Gecko) Version/7.2.1.0 Safari/536.2+

x-flash-version: 11,1,121,108

Connection: Keep-Alive

Referer: app:/PoliceScannerRadio.swf

Dictionary.com

Notes

- Sends PIN.

POST

/v2/word.json/perspicacious/complete?api_key=j9eXuBuiUK1T3Na&app_id=dcomCore_v32&device_id=0x24c13386&platform=Blackberry HTTP/1.1

Accept-Encoding: gzip,deflate

Proxy-Connection: Keep-Alive

Origin: local://

Accept-Language: en-US,en;q=0.8

User-Agent: Mozilla/5.0 (BB10; Touch) AppleWebKit/537.10+ (KHTML, like Gecko) Version/10.0.10.672 Mobile Safari/537.10+

Accept: application/json, text/javascript, */*; q=0.01

Host: restapi.dictionary.com

Connection: keep-alive

Content-Length: 0

GET

/v1/public/yql?q=select%20*%20from%20xml%20where%20url%3D%22http%3A%2F%2Fapi.dic

tionary.com%2Fv001%2Fdriver%2Findex.php%3Fvid%3D7CKHY134PPD5K590E3ONYNQ5FD0WY
VR68BO6DRA3GO%26type%3Dwordoftheday%26lang%3Den_US%26year%3D2013%26month%
3D4%26day%3D7%26platform%3DBlackBerry%26app_id%3Ddcombb10%22&format=xml'&call
back=jQuery1620036805661860853434_1365371173324&_=1365371175573 HTTP/1.1

Accept-Encoding: gzip,deflate

Proxy-Connection: Keep-Alive

Accept-Language: en-US,en;q=0.8

User-Agent: Mozilla/5.0 (BB10; Touch) AppleWebKit/537.10+ (KHTML, like Gecko)
Version/10.0.10.672 Mobile Safari/537.10+

Accept: */*

Host: query.yahooapis.com

Connection: keep-alive